Strategy Research Project

DON'T TOUCH MY BITS OR ELSE! – CYBER DETERRENCE

BY

LIEUTENANT COLONEL STEVEN D. REHN
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE
Don't Touch My Bits or Else! – Cyber Deterrence

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Steven D. Rehn

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lieutenant Colonel John A. Mowchan
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Can deterrence be effectively executed in cyberspace? Ultimately some aspects of deterrence as we understand it can be effective, but cyberspace is unique and complex enough that we must broaden our knowledge of deterrence and qualify its application to have any strategic effect within cyberspace. This paper will examine the concepts of deterrence theory, reflect on the environment and techniques that enabled nuclear deterrence, describe the cyberspace environment, contrast the two environments, discuss current deterrence policies and make recommendations on the applicability of deterrence in cyberspace.

15. SUBJECT TERMS
Cyber, Cyberwarfare, Cyberspace Operations, Deterrence Theory, Information Operations, National Security Strategy, Net Centric Warfare

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

DON'T TOUCH MY BITS OR ELSE! - CYBER DETERRENCE

by

Lieutenant Colonel Steven D. Rehn
United States Army

Lieutenant Colonel John Mowchan
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Steven D. Rehn

TITLE: Don’t Touch My Bits Or Else! - Cyber Deterrence

FORMAT: Strategy Research Project

DATE: 23 March 2011 WORD COUNT: 5,815 PAGES: 30

KEY TERMS: Cyber, Cyberwarfare, Cyberspace Operations, Deterrence Theory, Information Operations, National Security Strategy, Net Centric Warfare

CLASSIFICATION: Unclassified

Can deterrence be effectively executed in cyberspace? Ultimately some aspects of deterrence as we understand it can be effective, but cyberspace is unique and complex enough that we must broaden our knowledge of deterrence and qualify its application to have any strategic effect within cyberspace. This paper will examine the concepts of deterrence theory, reflect on the environment and techniques that enabled nuclear deterrence, describe the cyberspace environment, contrast the two environments, discuss current deterrence policies and make recommendations on the applicability of deterrence in cyberspace.

DON'T TOUCH MY BITS OR ELSE! - CYBER DETERRENCE

> Nobody is driven into war by ignorance, and no one thinks that he will gain anything from it is deterred by fear. The truth is that the aggressor deems the advantage to be greater than the suffering; and the side [that] is attacked would sooner run any risk than suffer the smallest immediate loss...[W]hen there is mutual fear, men think twice before they make aggressions upon one another.[1]
>
> —Thucydides

Thomas Schelling stated that deterrence at the highest level is "the threat intended to keep an adversary from doing something."[2] However, it is not just merely preventing an adversary from taking an action, but also influencing his understanding that the cost and risk associated with taking such an action are not to his advantage. As John Mearsheimer noted in *Conventional Deterrence* that "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[3] Deterrence proved to be an effective strategy during the Cold War preventing nuclear conflict. Can deterrence work in cyberspace? Ultimately some aspects of deterrence as we understand it can be effective, but cyberspace is unique and complex enough that we must broaden our knowledge of deterrence and qualify its application to have any strategic effect within cyberspace.

This paper will examine the concepts of deterrence theory, reflect on the environment that enabled nuclear deterrence, describe the cyberspace environment, contrast the two environments, discuss current deterrence policies and make recommendations on the applicability of deterrence in cyberspace.

In its simplest form, deterrence is to persuade someone (an enemy) not to do something they otherwise may have done.[4] The persuasion consists of an expression

(implied or overt) of intent or threat with consequences that create a prohibitive cost to the one considering the action. This persuasion is effective when the cost of the action becomes more than the actor is willing to bear. A threat alone is not sufficient to deter an action. The threat must also articulate the intent to protect a certain interest(s) and, more important, the ability to follow-through with the threat. William Kaufman asserted that, “Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability actually to achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him.”[5] Without credibility of the threat gained through demonstrated capability and the will to exercise that capability, deterrence has no chance of success. The enemy must be convinced the threat is real, you have the will to carry through the threat, and that it will inflict a cost to him. Schelling also pointed out that deterrence also includes an incentive— “involves a promise that abstaining from violence will remove the threat.”[6]

The ability to persuade is a cognitive function and relies upon human nature. Lawrence Freedman wrote, “plans may be hatched by the cool and calculating, but they are likely to be implemented by the passionate and the unpredictable.”[7] Deterrence relies on a psychological relationship whose goal is to shape an enemy’s perception, expectation, and ultimately his decision to take an action.[8] Reputations and past behavior matter, how we regard or attribute action today depends on what happened in the past.[9] What matters most is not our capability, but what the enemy believes our capability to be to execute that threat.[10] Ultimately the enemy determines whether or not

he is deterred and it is his conclusion whether or not he will accept the potential outcomes of his actions.[11]

Failures in deterrence are easily observed and are evident both at the time of failure and long after the fact. Deterrence successes are difficult to observe and can be unknown to those outside of the inner circle who are making the decisions. Leaders who choose to not act will be reluctant to publicize the true factors in their decision calculus for fear of being perceived as weak. In some cases deterrence may have been a factor, in others internal political or economic variables that have no relation to the actual deterrence problem may have weighed heavily in the decision not to act. Hence, any evidence of deterrence success is circumstantial and highly speculative.

Deterrence can be highly unpredictable. One must understand the social pressures of a potential enemy actor, his culture, and his self-perceived political and strategic position in order to effectively issue a threat of any real relevance. What seems like a credible threat may be subordinate to or even irrelevant to an enemy leader who fears the damage to his position, his family or his reputation should he not take action.[12] In the United States (U.S.) deterrence is based on the Western value of life and liberty; however, we must realize there are cultures that value stature and reputation over life where death is preferred over humiliation.[13]

Emanuel Adler wrote, “Deterrence strategy is a coercive social logic aimed at dissuading the use of violence.” [14] It rests on the premise that actors are: (1) rational; (2) understand the rules of the game; (3) engage in tacit and explicit exchange of information; (4) accurately assess the risks, costs, and gains of strategic games; (5) controls their emotions; and (6) hold normative assumptions about the appropriateness

and proportionality of military actions.[15] When any of these six elements fails to hold true on either side, the risk of conflict dramatically increases as ones side miscalculates or is playing a completely different strategic game than the other. Deterrence operates best when there is clarity in these elements, not when there is ambiguity which only increases the complexity.[16]

Complex deterrence, as described by T. V. Paul, is defined as “an ambiguous deterrence relationship, which is caused by fluid structural elements of the international system to the extent that the nature and type of actors, their power relationships, and their motives become unclear, making it difficult to mount and signal credible deterrent threats in accordance with the established precepts of deterrence theory.”[17] The environment becomes so complex; the likelihood that all parties have a similar view in line with Adler’s deterrence construct is highly unlikely, dramatically decreasing the success for deterrence.

Adler also points out that deterrence is dependent upon four basic assumptions. First, states are rational actors and they make cost-benefit calculations about whether to not pursue conflict.[18] He does acknowledge that rationality models differ in actors. Some operate on an ‘instrumental’ model, where they modify their goals to advance their self interest or obtain goods that maximize their utility. They will also modify their goals if the cost is perceived to be too high. Others operate under a ‘value’ model whereby they pursue intangible goals based on their values (e.g., self-respect, dignity, ethnic pride) with a high degree of commitment even when the cost is high and success is not assured.[19] Secondly, deterrence is used mainly by nation-states. Thirdly, that opponents would strike given the opportunity as intense rivalries exists among the parties. Finally,

each class of weapon is at a different layer in the deterrence calculus leading to response-in-kind, which aides in the discernment of threats and policies.[20]

If deterrence is anything that dissuades an attack, it is usually said to have two components: deterrence by denial (the ability to frustrate the attacks (defense)) and deterrence by punishment (the threat of retaliation (offense)).[21] The defenses in deterrence by denial "need not be perfect—only good enough to significantly complicate an adversary's planning to the point at which it becomes impossible to carry out an attack with a high probability of success," as noted by John Steinbruner.[22] Deterrence by punishment has been the U.S. core national security doctrine since the 1950's. If you do us harm, even greater harm will befall you.[23]

Nuclear Deterrence Environment

Deterrence theory and practice came to its pinnacle during the Cold War. It prevented nuclear conflict because it was singular and symmetric. Singular in that the prospect of nuclear conflict was so frightening that no one dared to invoke it—mass destruction on a global scale. Symmetric in that the capabilities were equivalent on both sides as each had the ability to not only survive a first round strike, but inflict massive retaliation on the initiator providing no clear advantage for launching the first strike. Myriam Dunn Cavelty pointed out that "the end of the Cold War not only brought an end to the relatively stable bipolar world order but also the end of the relatively bounded nature of threats."[24] The nuclear environment was known and fairly predictable with relatively stable components.

Experts on deterrence theory agree that nuclear deterrence worked during the Cold War primarily because the two key players, the United States and the Soviet

Union, understood and operated within the construct described by Adler. In particular each made declarative policies that communicated their intentions in regards to nuclear weapons. In *The Evolution of Deterrence 1945–1958*, William Kaufmann points out that an intention includes two parts: “an expressed intention” and a “certain interest.” The first part is a declaratory policy that makes clear what is to be deterred.[25] Defining a certain interest can and is more often more ambiguous.

As pointed out earlier, Adler’s six elements provide a framework to understand the nuclear environment in context. The world was bipolar, with the United States and the Union of Soviet Socialist Republic (U.S.S.R.) on opposite sides, each whose primary interest was its own survival while operating under an instrumental value model. The risk of nuclear conflict was characterized by the shear destructive power of the weapons; the potential for punishment was beyond the ability for any nation to absorb and tamed most statesmen.[26] Both sides clearly understood the rules of the international strategic game. There were no viable second or third moves; everything rested on the first move which is why, in part, no one wanted to make that first move.[27] Through a series of arms-control negotiations and diplomatic engagements, communication between the U.S. and U.S.S.R. was open and frank.[28] The open dialogue prevented any confusion or misinterpretation of the other’s intentions and willingness to act, making deterrence a viable option.

The nuclear environment consisted of state-centric actors. It was reasonable to presume that only nation-states possessed the technology and could afford to build the infrastructure, warheads, and delivery mechanisms required for nuclear weapons.[29] Each side possessed the ability to understand each other’s capabilities and maintain

sufficient knowledge of their weapons posture enabling them to formulate an assessment on the risk a nuclear adversary posed at any given time. This was achieved through capabilities that could determine the number of nuclear weapon systems, origin of development, their yields, and launching point of delivery vehicles.[30] The environment also presumed that there were unitary actors such that the nuclear forces were under the direction and control of the state government and used in accordance with its national leaders' objectives.[31]

Cyber Deterrence Environment

Cyberspace is an environment that is in a constant state of change where time and distance become irrelevant.[32] Thousands of devices are added, removed, or reconfigured to alter the very nature of the landscape and the way they interact within the domain, reducing predictability. Myriam Dunn Cavelty likened this as, "a state of never being but always becoming."[33] Only milliseconds separate the interactions of any nodes at disparate geographical locations throughout the world. In no other domain can an action have an effect thousands of miles away in less than a second. For potential adversaries any potential target is only 20 microseconds away.[34] The only limiting factor is the intended target must be connected to the logical network. States with a greater dependency on networked information systems are at greater risks to the effects of cyber attacks. Today, many nations acknowledge the dependency on cyberspace as evidenced in the United Kingdom's National Security Strategy: "It (cyberspace) is integral to our economy and our security and access to the internet, the largest component of cyberspace, is already viewed by many as the 'fourth utility', a right rather than a privilege."[35]

Conflict in cyberspace is highly asymmetric. The cost of entry to procure a cyber capability—a tool or weapon—can be very low yet the cost and impact borne by the victim of his attack can be very high.[36] In the other domains, the cost of entry to conduct attacks is significant and precludes most non-state actors from posing a significant threat to states without resourcing from another state. With a lower cost of entry, the number of actors in cyberspace is exponentially higher creating a multi-polar world that combines threats from both nation-states and non-state actors. It is conceivable that an individual can cause great damage to a nation-state to a degree never before seen. "Gone are the days when one needed to raise an army, build a command structure, train soldiers, and purchase weapons to attack an adversary," as noted by Frank J. Cilluffo and J. Paul Nicholas.[37]

Furthermore, the absence of immediate, visible harm and physical damage can mean that cyber attacks are regarded as somewhat removed from reality.[38] The effects from both nuclear and conventional weapons are known and can be visibly seen and understood not only by those who practice war, but even those who have no familiarity with the aspects of war. The effects from cyber attacks are often not visible to the naked or untrained eye. There is no explosion or cloud of smoke to indicate the weapon was used. Even when the effects are observed, determining the damage caused by a cyber weapon and not a 'system error' or accidental act is difficult and time consuming. Not only are the effects difficult to trace to a cyber weapon, but the fundamental nature of the threat to national security remains largely hypothetical.[39]

Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the target's vulnerabilities with permanent effects hard to

produce.[40] Attacks methods that work today may not work tomorrow, as defenders recognize the vulnerability and take actions to mitigate the risk. In the physical domain, a weapon system is optimized for a specific type of target(s) for maximum effect. If a weapon is used against a target it was not intended for, it may not produce the desired effect; however, it will cause some effect. In cyberspace, because attacks depend on exploiting vulnerabilities, specific exploits must be used that are tailored to a specific target system using a specific application with a specific version for any effect to be achieved. In essence, cyber weapons are tailor made for specific targets with a limited shelf life since vulnerabilities are constantly being discovered and corrected. Additionally, the cyberspace landscape is in constant change with the application of patches, systems added or removed, configuration updates, and network topologies altered. The target space today is different than that of yesterday; one simple change can make a cyber weapon completely ineffective. There is, in the end, no forced entry in cyberspace.[41] Follow-on attacks against the same enemy will most likely require new weapons, as the vulnerability exploited will frequently be identified and repaired rendering the initial weapon no longer effective.

Within cyberspace, infrastructure, technology, and background knowledge are easily and widely available to all: nation-states, non-state actors, public and private companies and even private individuals.[42] It is difficult to identify an attack as crafty adversaries will conceal their attacks in the 'noise' of normal traffic. Even when an attack is identified, it is difficult to attribute responsibility to a particular actor. It is even harder to conclude with a certainty that the actor was operating as a result of a national decision by a nation-state.[43]

Nuclear vs Cyber Deterrence

Steinbruner claimed, “although nuclear weapons and cyber weapons share one key characteristic (the superiority of offense over defense), they differ in many other key characteristics…nuclear deterrence and cyber deterrence do raise many of the same questions, but indeed that the answers to these questions are quite different.”[44] Nuclear deterrence was based on several key elements: Attribution (understanding the identity of the attacker and their motive), location (knowing where a strike came from), response (being able to respond, even if attacked first), and transparency (the enemy’s knowledge of our capability and intent to counter with massive force).[45] In the nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible; there were no third parties to consider; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose.[46] These aspects of deterrence all present a challenge with respect to cyber deterrence.

The tools cyber actors can employ are almost always anonymous—a defender can sometimes learn where an attack came from, but such an attempt is often time-consuming. That means “attribution” in cyberspace is costly and comparatively rare.[47] Amit Sharma asserts that, “the technical limitations of attribution, which prevents the victim of a cyber-attack from identifying their attacker in cyberspace, meaning a potentially anonymous aggressor, cannot be deterred.”[48]

In conventional and nuclear conflicts, it was fairly evident to ascertain who was responsible for attacks based on location of attack, capabilities and detection and

tracking of the attack while underway. Only so many nations have the ability to launch an Inter-Continental Ballistic Missile from known fixed sites where the launch can be observed and detected. Even with air or sea launched weapons, it could be easily deduced who was responsible based on the location of launch and impact, weapon capability, and the tracking of the platforms and weapons. Assuming that a nuclear weapon did explode without warning, the isotopal analysis would allow for attribution to the responsible state.

This level of attribution is not easily achieved in cyberspace. According to some reports, computer systems from more than one hundred countries were involved in the attacks on Estonia in 2007.[49] The Estonians reported that some of the earliest salvoes came from computers linked to the Russian government, but most of them came from thousands of ordinary computers all over the world. Some of these were run by private citizens who disagreed with Estonia's position.[50] Even though some computers appeared to be linked to the Russian government, there was no evidence that Moscow had willfully participated in the attack as their systems could have been penetrated and subverted as part of the network of attacking nodes against Estonia. Thus, even when an attack can be traced to a geographic location, the fact that it is part of the logical network and can be utilized by a plethora of cyber actors under the influence of multiple personas (a many-to-many relationship) makes attribution extremely difficult.

State attribution remains difficult even if the nationality of the individual responsible for the attacks is known. For example, even if the attack on Estonia was traced to a Russian citizen, there may not be any evidence linking the perpetrator to the Russian government. Because the cost associated with most large-scale conventional

and nuclear attacks is so high and require inordinate amount of support, state sponsorship in these actions is required. However, due to the low cost of entry into cyberspace, state sponsorship is not required and should not be assumed. Hence, attributing state involvement, the key questions are (a) did a person act as an agent of a particular state and (b) do his actions qualify as actions of that state.[51] Just because an individual is an agent of a state, his actions may not be sanctioned by that state. These two questions are extremely difficult to answer and must be, or at least credible enough for the international community to believe.

Martin Libicki asserts that, “True, ironclad attribution is not necessary for deterrence as long as attackers can be persuaded that their actions may provoke retaliation. Yet some proof may be necessary given (1) that the attacker may believe it can shake the retaliator’s belief that it achieved attribution by doing nothing different (“who, me?”) in response to retaliation, (2) that mistaken attribution makes new enemies, and (3) that neutral observers may need to be convinced that retaliation is not aggression.”[52] Thus attribution is cyberspace is something that very few states have made formal challenges to, but have informally acknowledged or placed on notice other states activities. Germany’s Chancellor, Andrea Merkel, felt confident enough to complain in person to China’s Premier Wen Jiabao of the attributed activities of China’s People’s Liberation Army (PLA) activities to infect and extract data from Germany’s networks in August 2007.[53]

The lower the odds are of attribution the increased likelihood of an attack which would call for a higher penalty to convince an attacker that the cost of carrying out the attack is too great to pursue. Unfortunately in cyberspace there are no smoldering

buildings or loud explosions to easily convince third parties an attack actually occurred. Furthermore, there is no easy way to understand the extent of damage caused by the attack. Therefore any overt punishment pursued by the attacked, may be seen as disproportionate placing the attacker as the victim in the eyes of the international community.

"Mutual assured destruction" principle does not translate well in cyberspace. There is limited ability to inflict physical damage or incite political instability against an attacker who does not possess physical assets or have a population to create instability as in the case of non-state actors. For those state actors who are not dependent upon information technology for their economic or social well-being there is very little to counter-attack in cyberspace and any response-in-kind threat is not valid to deter an aggressor. One must also consider the perception of the international community condoning a disproportional response against a disadvantaged actor who attacks a state of technologic superiority.

Nuclear deterrence was based primarily on deterrence by punishment as the response would be equally as harmful as the original attack. In cyberspace, the limits of deterrence based on retaliation lead one to focus on deterrence by denial.[54] However, there is no true denial within cyberspace other than to completely disconnect and power down the systems to preclude an attack on the system. Doing so would also deny us the use of that system and may achieve the very effect the attacker desired.

Deterrence by denial leads one to invest in a defensive strategy. By making our systems appear as impregnable, an attacker would be deterred because the cost to find and understand the vulnerabilities to exploit the system is too high. That cost can either

be time, resources required or the risk of being caught and exposed to the international community. The cost for an attacker are far less than that of the defender who must invest in reducing all his vulnerabilities, while an attacker can focus on exploiting a select few to be successful.

Experience has shown that strengthening a system's defensive posture discourages most attackers, but only delays determined adversaries. The loss of time and the uncertainty of success are the costs the attacker must consider in order to continue the attack and can contribute to deterrence provided it places at risk the ability for an adversary to meet his timetable.[55]

The similarities between cyber attack and cyber espionage presents a challenge for deterrence by denial.[56] An attacker can refute any claims against it and state there was no intent to deny or degrade data, but only to access and obtain the data—cyber espionage. While cyber espionage is an act the international community may condone, it is not likely any serious actions would be taken against state actors since it is espionage—an internationally accepted behavior and cyber espionage is only an extension of that established norm.

Patrick M. Morgan identified that in cyberspace, "the nature of the opponents is certainly very different…in the Cold War the enemies were 'out there,' beyond the nation's boundaries, cyberspace is transnational. Thus the enemy is in here operating with us in cyberspace.[57] Myriam Dunn Cavelty stated, "Cyber-threat politics take place in a security environment that is [now] governed by the notion of risk management rather than traditional security practices, and the strategies and policies pursued to secure the information space change the role of government in providing security;

providing security inside a society is not the same as on the outside."[58] The traditional methods of providing security have changed. Those who previously provided internal security of the state are finding themselves more involved with international security matters, policies and authorities, and vice versa.

Declarative Statements

An effective deterrence policy must articulate the intention to protect a certain interest(s). Current U.S. polices acknowledge the critical role and function cyberspace plays in our global economic and national well-being, and for the first time states the U.S. is willing to protect cyberspace. The 2010 National Security Strategy (NSS) declares, "Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority."[59] But do current U.S. declarative statements in regards to cyberspace convey the commitment by the United States to deter aggression against those interests?

The U.S. Strategic Command defines deterrence as the ability to, "convince adversaries not to take actions that threaten U.S. vital interest by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."[60] The 2011 National Military Strategy (NMS) acknowledges that, "Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques, while also providing potential adversaries acceptable alternative

courses of action."[61] Thus the United States continues to acknowledge and promote a deterrence strategy.

In current U.S. policy, nuclear deterrence is achieved through the 2010 National Security Strategy, "As long as any nuclear weapons exist, the United States will sustain a safe, secure, and effective nuclear arsenal, both to deter potential adversaries and to assure U.S. allies and other security partners that they can count on America's security commitments."[62] It is further detailed in the 2010 Nuclear Posture Review which states, "deterrence of nuclear attack on the United States or our allies and partners [is] the sole purpose of U.S. nuclear weapons; only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States or its allies and partners; and [the U.S.] will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the NPT and in compliance with their nuclear nonproliferation obligations."[63] The Nuclear Posture Review provides explicit details on U.S. intentions with respect to the use of nuclear weapons. What constitutes "vital interests" is left to interpretation beginning with the general interest of security, prosperity, values and international order defined in the NSS. It is fairly clear when the U.S. would use nuclear weapons, but not necessarily what constitutes the extreme circumstances to protect which vital interests.

Having a somewhat vague public policy is not necessarily detrimental in deterrence. Some ambiguity complicates the cost analysis an adversary undergoes to determine whether or not to pursue an attack. Hence, an adversary is likely to refrain from any action that may possibly invoke nuclear punishment even if he doesn't

necessarily know exactly what level of action does not invoke a nuclear response. The mere threat of a possible nuclear retaliation is enough to deter his action.

The need for similar declarative statements in regards to cyberspace is recognized, but such statements are just now beginning to formulate and begin to find their way into national policy statements. In January 2010, Secretary of State Hillary Clinton stated, “States, terrorists, and those who would act as their proxies must know the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation.”[64] This is further reinforced in the current 2011 NMS which states, “Should a large-scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable.”[65]

These statements acknowledge the threat to and importance of protecting cyberspace, but lack the clarity that signals the U.S. intends to defend cyberspace, if necessary, with force. However, they do provide a wide range of response options an adversary must consider. Will the U.S. respond with force, diplomatically, or possibly with economic sanctions? The NMS states, “To safeguard U.S. and partner nation interests, we will be prepared to demonstrate the will and commit the resources needed to oppose any nation’s actions that jeopardize access to and use of the global commons and cyberspace, or that threaten the security of our allies.”[66] Again, one must assume the degree of punishment the U.S. is willing to impose. Albeit, the U.S. is one of the first

countries to declare that cyberspace is in its national interest and it is willing to commit resources to ensure access.

The creation of the United States Cyber Command sends a strong signal to the world the U.S. not only intends to defend cyberspace, but is also building the capability to execute full spectrum military cyberspace operations and integrating cyberspace operations and synchronizing warfighting effects across the global environment (much as it does in other mission areas).[67] In time, Cyber Command will have demonstrated the capability to inflict a cost sufficient to deter an attacker either through denial or response. This leaves a key question in one's mind: Does the U.S. have the national will to respond to a cyber attack? The declarative policies should be strong enough to convince an adversary that we do have the will and the means, while leaving open the options of which type of particular response. An open set of options complicates a potential adversaries decision process by making the cost vs. benefit of an attack calculation more difficult, which in turns may make him more apprehensive to pursue the attack not knowing how the attacked may respond.

Mary Ann Davidson testified to Congress in March 2009 that the U.S. should institute a Monroe-like doctrine for cyberspace. She argued that having such a doctrine would, "signal to foreign powers that the U.S. had territorial sphere of influence and that incursions would be met with a response."[68] It would prove flexible, yet powerful, in that it was specific enough to state our interest while not specifying all possible responses in advance. She also professed that, "any consideration of our cyber interest must be evaluated within the larger view of our national security concerns and our freedoms."[69]

A Monroe-like doctrine for cyberspace is a start and the 2011 NMS begins to lay out that strategy.

Conclusions

Patrick M. Morgan stated, “Deterrence has to be achieved not by making a response highly likely but via the possibility of one… in deterrence such threats can be effective not in preventing all attacks but in reducing the highly provocative ones.”[70] Deterrence in cyberspace will depend on our ability to defend our networks and provide an appropriate response—deterrence by denial and punishment. We will make a costly mistake if we limit ourselves to only respond-in-kind and must use all the elements of national power at our disposal. As Davidson professed, “deterrence strategy needs to have teeth to be credible, or it becomes a paper tiger.”[71]

Investments in the ability to identify and attribute attacks are required; we cannot let these current capability shortfalls preclude the formulation of a deterrence strategy. As in nuclear deterrence, similar capabilities did not exist when nuclear weapons first appeared, but evolved over time as the strategic needs became understood. We must acknowledge and understand the dangers lack of attribution presents in our response actions and formulate and adjust our deterrence strategy accordingly.

As current cyber attacks occur daily, linkage to political agendas of nation-states has generally not yet occurred. Cyberspace as a global common must be brought to the forefront of international discussions in order to establish norms and acceptable behavior. These international discussions will help clarify and qualify the key elements Adler identified for effective deterrence as they currently are ambiguous, or not directly applicable in cyberspace. There are international organizations, such as The Council of

Europe's Convention on Cybercrime, that are attempting to establish the acceptable norms within cyberspace. While this is a good start, these organizations are focusing on criminal activity and not what constitutes an act of war. Nation-states must engage in dialogue to decide what constitutes an attack that threatens national security. They must establish mechanisms to indentify and inform each other of attacks to preclude unwarranted retaliation and disproportional response.

Governments alone cannot effectively create deterrence in cyberspace. They must act in coordination and cooperation with civilian entities (e.g., critical infrastructure, the Defense Industrial Base, economic and trade institutions, commercial industry, and academia) since much of the cyber domain is operated and maintained by the private sector. If deterrence by denial is to have any chance of success, information sharing and a collective defense between government and non-government entities is critical.

Nation-states must be willing to seek response options beyond military actions to cyber events that may not cross the threshold for an act of war, but damage their national interest. These actions may be diplomatic, economic, or information. For example, a state may impose economic sanctions or make public allegations leading to international admonishment against states which commit cyber attacks. Established partnerships and collective defense of cyberspace will enhance the trust between states and provide for mutual support for such events. Collective defense between states will also complicate the attacker’s decision process as he must now consider the combined capabilities of the each state in his decision of whether to launch a cyber attack.

Cyberspace deterrence is a complex form of deterrence that requires extensive thought and analysis to develop a strategy that achieves the desired outcomes. Nuclear

deterrence was formulated over the course of the Cold War and continues to evolve today. Although the environments are radically different, the lessons of nuclear deterrence can guide the development of cyber deterrence. Some nuclear deterrence strategies can be applied in cyberspace, while others cannot. We must start by clearly declaring our willingness to protect cyberspace and the extent to which we will undertake to ensure access to and the integrity of information contained within cyberspace is maintained.

Endnotes

[1] Thucydides, *History of the Peloponnesian War*, Benjamin Jowett, trans. (Amherst, NY: Prometheus Books, 1998), 59-62, quoted in Austin Long, *Deterrence from the Cold War to the Long War* (Santa Monica, CA: RAND Corporation, 2008), 5.

[2] Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1967), 69.

[3] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 14.

[4] Colin S. Gray, "Gaining Compliance: The Theory of Deterrence and its Modern Application," *Comparative Strategy*, *29:3* (2010), 278.

[5] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 7.

[6] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 7.

[7] Lawrence Freedman, *The Transformation of Strategic Affairs*, *Adelphi Paper 379* (London, UK: Routledge, 2006), 36.

[8] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: The National Academies Press, 2010), 56, http://www.nap.edu/catalog/12997.html (accessed February 9, 2011).

[9] John D. Steinbruner, "Reprinted Letter Report from the Committee on Deterring Cyberattacks, March 25, 2010," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: The National Academies Press, 2010), 350, http://www.nap.edu/catalog/12997.html (accessed February 9, 2011).

[10] Gray, “Gaining Compliance: The Theory of Deterrence and its Modern Application,” 278-279.

[11] Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” 61.

[12] Gray, “Gaining Compliance: The Theory of Deterrence and its Modern Application,” 280.

[13] Emanuel Adler, “Complex Deterrence in the Asymmetric Warfare Era,” in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago and London: University of Chicago Press, 2009), 95.

[14] Ibid., 88.

[15] Ibid.

[16] T. V. Paul, “Complex Deterrence: An Introduction,” in *Complex Deterrence: Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago and London: University of Chicago Press, 2009), 8.

[17] Ibid., 8.

[18] Ibid., 5.

[19] Ibid., 6.

[20] Ibid., 7.

[21] Libicki, *Cyberdeterrence and Cyberwar*, 7.

[22] Steinbruner, “Reprinted Letter Report from the Committee on Deterring Cyberattacks, March 25, 2010,” 354.

[23] General Eugene E., Habiger, USAF (Ret.), “Cyberwarfare and Cyberterrorism: The Need For A New U.S. Strategic Approach,” *Provoking Cybersecurity Change White Paper Series* (n.p.: The Cyber Secure Institute White Paper 1:2010, February 1, 2010), 2, http://cybersecureinstitute.org/ docs/whitepapers/Habiger_2_1_10.pdf (accessed December 13, 2010).

[24] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics U.S. Efforts to Secure the Information Age* (London and New York: Routledge, 2008), 139.

[25] William W. Kaufmann, *The Evolution of Deterrence 1945–1958* (Santa Monica, CA: RAND Corporation, October 20, 1958) quoted in Austin Long, *Deterrence from the Cold War to the Long War* (Santa Monica, CA: RAND Corporation, 2008), 8.

[26] Forsyth, Saltzman, and Schaub, "Minimum Deterrence and Its Critics," 5.

[27] James Wood Forsyth, Jr., B. Chance Saltzman, and Gary Schaub, Jr., "Minimum Deterrence and Its Critics," *Strategic Studies Quarterly 4*, no. 4 (Winter 2010), 7.

[28] T. V. Paul, “Complex Deterrence: An Introduction,” 9.

[29] Steinbruner, “Reprinted Letter Report from the Committee on Deterring Cyberattacks, March 25, 2010,” 351.

[30] Ibid., 352.

[31] Ibid., 351.

[32] General Keith B. Alexander, “U.S. Cyber Command: Organizing For Cyberspace Operations,” *Statement Before The House Committee On Armed Services* (September 23, 2010), 4, http://armedservices.house.gov/index.cfm/files/serve?File_id=040616f9-4c7a-470a-b2ad-587761d7ef28A01 (accessed December 13, 2010).

[33] Cavelty, *Cyber-Security and Threat Politics U.S. Efforts to Secure the Information Age*, 141.

[34] Mary Ann Davidson, “The Monroe Doctrine in Cyberspace,” *Testimony before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology* (March 10, 2009), http://www.whitehouse.gov/files/documents/cyber/Davidson%20MaryAnn%20-%20The%20Monroe%20Doctrine%20in%20Cyberspace.pdf (accessed November 22, 2010).

[35] Prime Minister David Cameron, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: October 2010), 29.

[36] Alexander, “U.S. Cyber Command: Organizing For Cyberspace Operations, Statement Before The House Committee On Armed Services,” 4.

[37] Frank J. Cilluffo and J. Paul Nicholas, “CYBERSTRATEGY 2.0,” *The Journal of International Security Affairs*, *Spring 2006 - Number 10*, http://www.securityaffairs.org/issues/2006/10/cilluffo_nicholas.php (accessed January 11, 2011).

[38] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *On Cyber Warfare* (London: The Royal Institute of International Affairs, November 2010), 10.

[39] Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” 58.

[40] Libicki, *Cyberdeterrence and Cyberwar*, iii.

[41] Ibid., xiv.

[42] Steinbruner, “Reprinted Letter Report from the Committee on Deterring Cyberattacks, March 25, 2010,” 351.

[43] Ibid.

[44] Ibid., 350.

[45] Mike McConnell, “To Win the Cyber-War, Look to the Cold War,” *Washington Post*, 28 February 2010, http://www.boozallen.com/media/ file/20424-WP-McConnell-02282010.pdf (accessed November 5, 2010).

[46] Libicki, *Cyberdeterrence and Cyberwar*, xvi.

[47] Alexander, “U.S. Cyber Command: Organizing For Cyberspace Operations, Statement Before The House Committee On Armed Services,” 4.

[48] Samaan, "Cyber Command: The Rift in U.S. Military Cyber-Strategy," 18.

[49] Marco Gercke, “Wild Wild Web,” *The European Magazine,* January 5, 2011, http://www.theeuropean-magazine.com/148-gercke-marco/161-the-reality-of-cyberwars (accessed January 14, 2011).

[50] "Europe: A cyber-riot; Estonia and Russia," *The Economist*, May 12, 2007, 42, http://www.proquest.com.ezproxy.usawcpubs.org/ (accessed January 14, 2011).

[51] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, “Cyber Attacks Against Georgia: Legal Lessons Identified,” (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), 22, http://www.carlisle.army.mil/DIME/documents/ Georgia%201%200.pdf (accessed January 5, 2011).

[52] Libicki, *Cyberdeterrence and Cyberwar*, xvi.

[53] Ibid., 25.

[54] Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” 59.

[55] Steinbruner, “Reprinted Letter Report from the Committee on Deterring Cyberattacks, March 25, 2010,” 355.

[56] Cyber Espionage is defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Although many actions of cyber espionage are the same steps as a cyber attack, a cyber attack will add additional steps to modify or deny the user access to data and/or full use of their system, while cyber espionage allows the user to maintain access to their data.

[57] Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” 58.

[58] Cavelty, *Cyber-Security and Threat Politics U.S. Efforts to Secure the Information Age*, 140.

[59] Barrack Obama, *National Security Strategy* (Washington, D.C.: The White House, May 2010), 27.

[60] U.S. Department of Defense, *Deterrence Operations: Joint Operating Concept, Version 2.0* (Washington, D.C.: DoD, December 2006), 350, http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc (accessed November 12, 2010).

[61] M. G. Mullen, *The National Military Strategy of the United States of America, 2011, Redefining America's Military Leadership* (Washington, D.C.: Chairman of the Joint Chiefs of Staff, February 08, 2011), 8, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed 10 February 10, 2011).

[62] Obama, *National Security Strategy*, 23.

[63] Department of Defense, *Nuclear Posture Review Report* (Washington, D.C.: Department of Defense, April 2010), ix.

[64] Secretary of State Hillary Clinton, Remarks of the Secretary on Internet Freedom, delivered January 21, 2010 at the Newseum, Washington, D.C.

[65] Mullen, *The National Military Strategy of the United States of America, 2011, Redefining America's Military Leadership*, 10.

[66] Ibid., 14.

[67] Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academy Press, 2010), 252.

[68] Davidson, "The Monroe Doctrine in Cyberspace," 3.

[69] Ibid.

[70] T. V. Paul, "Complex Deterrence: An Introduction," 8.

[71] Davidson, "The Monroe Doctrine in Cyberspace," 4.